

FILED 8 MAR '18 10:10USDC-ORP

AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))The person of Kevin John Myers and the premises
located at 2300 NW Rolling Green Drive, Apt. 126,
Corvallis, OR 97330, described in Attachment A)

Case No.

'18-MC-184

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the _____ District of _____ Oregon _____ (identify the person or describe property to be searched and give its location):

The person of Kevin John Myers and the premises located at 2300 NW Rolling Green Drive, Apt. 126, Corvallis, OR 97330, more fully described in Attachment A hereto.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See Attachment B hereto.

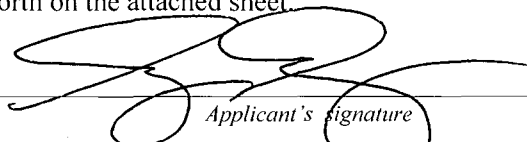
The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252A, and the application is based on these facts: See the attached affidavit of Special Agent Seung Sung, U.S. Department of Homeland Security, Homeland Security Investigations (HSI),

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Seung Sung, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: March 8, 2018

City and state: Portland, Oregon



Judge's signature

Honorable John V. Acosta, U.S. Magistrate Judge

Printed name and title

STATE OF OREGON)
) ss. AFFIDAVIT OF SEUNG SUNG
County of Multnomah)

I, Seung Sung, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) for the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), in Portland, Oregon. HSI is responsible for enforcing the customs laws, immigration laws, and federal criminal statutes of the United States. I am a law enforcement officer of the United States, and I am authorized by law to conduct investigations and to make arrests for felony offenses.

2. I have been a special agent with HSI since July 2002. My duties include the enforcement of federal criminal statutes prohibiting the sexual exploitation of children, including Title 18, United States Code, Sections 2251 through 2259, the Sexual Exploitation of Children Act (SECA). I have worked with agents involved in numerous investigations involving the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of premises and assisted in gathering evidence pursuant to search warrants, including search warrants in multiple child pornography investigations. I graduated from the Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training, both held at the Federal Law Enforcement Training Center.

3. This affidavit is submitted in support of an application for a search warrant authorizing searches of the person Kevin John MYERS (date of birth XX-XX-1966), and his residence, located at 2300 NW Rolling Green Drive, Apt. 126, Corvallis, Oregon 97330, more

fully described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A, as set forth in Attachment B.

4. The facts set forth in this affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of an application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

Statutory Authority

5. Title 18, United States Code, Section 2252A(a)(1) prohibits a person from knowingly transporting or shipping child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

6. Title 18, United States Code, Sections 2252A(a)(2) and (b)(1) prohibit a person from knowingly receiving or distributing any material containing child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or conspiring or attempting to do so.

7. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or accessing with intent to view any child pornography that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting

interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempting to do so.

Definitions

8. The following definitions apply to this affidavit and to Attachment B:

a) “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b) “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in children but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c) “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d) “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

e) “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

f) “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

g) “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

h) “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) the lascivious exhibition of the genitals or pubic area of any person.

i) “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Background on Computers and Child Pornography

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the knowledge, experience, and training of other law

enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have dramatically changed the manner in which child pornography is produced and distributed.

10. Digital cameras and video recorders (including those found on many smart phones) readily and easily allow for the production of child pornography. Using digital cameras or video recorders, images and videos of child pornography can be uploaded directly onto a computer, where they can easily be edited, manipulated, copied, and distributed. A paper photograph can be digitized and uploaded to a computer through the use of a scanner. Once uploaded, such photographs can be edited, manipulated, copied, and distributed just like any other digital image. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to millions of computers around the world.

11. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, a wide variety of removable digital data storage media exist which add additional storage capacity, and which provide a portable platform on which to store and transport child pornography. Examples of such removable storage media include external hard drives, thumb drives, flash drives, and secure digital data cards, some of which are quite small, are highly portable, are easily concealed, and are often carried on a subject's person. Smart phones are also often used to access the Internet, and to produce, transport, receive, store, and view child pornography. An

individual using a smart phone can easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Smart phones are relatively small, are highly portable, and are often carried on a subject's person.

12. The Internet affords individuals who collect and trade in child pornography several different venues for meeting each other, and for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Such venues include chat rooms, bulletin board services, social networking sites, instant messaging services, and peer-to-peer (P2P) file sharing networks.

13. Individuals also use online resources to store and retrieve child pornography, including services offered by Internet portals such as Yahoo!, Hotmail, Google, and others. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

14. Typically, computers or devices on the Internet are referenced by a unique Internet Protocol (IP) address, much like a telephone has a unique telephone number. Each time an individual accesses the Internet, the computer or device from which that individual initiates access is assigned an IP address by the individual's Internet Service Provider. An IP address may be statically assigned, meaning the individual is assigned the same IP address each time he or she accesses the Internet. An IP address may also be dynamically assigned, meaning that a user may receive a different IP address each time he or she accesses the Internet. Internet service

providers typically log the date, time, and duration of the Internet session for each IP address and can identify the subscriber of that IP address for such a session from those records.

15. Based on my training and experience, and the training and experience of other investigators with whom I have spoken, I know that individuals who collect and trade in child pornography frequently store their collections on computers and digital storage media, which they keep in secure locations, such as their residences. Such persons typically keep their collections of child pornography close at hand, and often retain their collections for extended periods of time. Such persons treat their collections as prized possessions, rarely disposing of them entirely. In some recent cases, however, such persons have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection indefinitely.

16. Digital information, including communications to and from a computer, is often saved or stored on a computer. Storing this information can be intentional, for example by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. For example, a forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or

viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

17. When a person deletes a file on a computer, the data contained in the file ordinarily does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

18. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in collecting and trading child pornography:

a. Those who collect and trade child pornography over the Internet often maintain their collections that are in a digital or electronic format in a safe, secure, and private

environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

b. Such persons also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of the names of, and contact information for, individuals with whom they have been in contact and who share the same interests in child pornography.

c. Such persons prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

d. In the case of those who collect and trade child pornography via email, the nature of email itself provides a convenient means by which these individuals can access their collections from any computer, at any location with Internet access. These individuals therefore do not need to physically carry their collections with them, but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers that allow users to store a large amount of material at little or no cost, thus eliminating the need to store child pornography collections on the users' own computers.

Information on the Chatstep Messaging Service

19. Chatstep.com ("Chatstep") is a free online chat service that allows users to create or join public or private chat rooms. To use Chatstep, a user simply creates a user name and selects the chat room he or she wants to enter. Private chat rooms generally require a password to enter. Once in a chat room, the user can chat with the entire room or individually with other

users in the room. Moreover, a user can upload files to share with the room, making those files visible to all occupants. Individuals may enter chat rooms to discuss a variety of topics, including sexual fetishes or a sexual interest in children. No registration is required to use Chatstep.

20. Users select their own user name, or nickname, when entering a chat room. Two different users can use the same nickname unless they are in the same chatroom at the same time. In addition, a single user may be in multiple chat rooms at the same time, using a different nickname for each room.

21. Chatstep does not store copies of chat messages, files, or images. However, when a user joins a chat room, Chatstep logs the user's nickname, IP address, port number, the room name, and the date and time. When a user uploads an image, it is automatically checked against Microsoft PhotoDNA, which is a system for detecting and reporting contraband images. If a match is detected, the picture is blocked from being shared and the image and IP address of the uploading user is automatically reported to the National Center for Missing and Exploited Children (NCMEC). Chatstep employees do not manually review images or videos before the images and/or videos are reported to NCMEC, nor do they monitor rooms looking for contraband images/videos. Only images recognized as contraband by PhotoDNA are reported to NCMEC.

The NZDCET and HSI Investigation

22. In October 2016, HSI special agents in Phoenix, Arizona, became involved in an ongoing child pornography investigation with investigators from New Zealand Department of Internal Affairs Digital Child Exploitation Team (NZDCET). The investigation involves

numerous people living in various countries, including the United States, who use Chatstep to distribute and/or collect images and videos depicting the sexual exploitation of children. Users can post images directly into a chat room, or can post hyperlinks that direct the user to images and videos stored elsewhere on the Internet.

23. In addition to posting images or videos (or hyperlinks to images or videos), users discuss various topics in the chat rooms. Topics include the possible presence of law enforcement officers in chat rooms, how best to distribute or share image files, how to mask users' true identities, and how to avoid Chatstep's automatic reporting protocols. Investigators have seen users deliberately modify links to files containing child pornography, such that other users must correct the modification (often a matter of correcting a common misspelling or removing an extraneous character) before the link will actually work.

Statement of Probable Cause

24. On or about August 25, 2017, an NZDCET investigator, acting in an undercover capacity, observed multiple individuals accessing a Chatstep chatroom called "Ghotel." On August 25, 2017, at 4:08 am UTC (Universal Time Coordinated), the NZDCET investigator saw a user with the nickname "Dairy" post a link that contained twelve image files depicting suspected child pornography. The NZDCET investigator clicked on the link and downloaded the image files. The NZDCET investigator captured a screenshot of the "Ghotel" chat room after "Dairy" posted the link. The investigator also captured a screen shot of the suspected child pornography images that appeared when the investigator clicked on the link that "Dairy" posted.

25. On August 25, 2017, the NZDCET investigator requested from Chatstep IP address records for Chatstep user "Dairy" in the "Ghotel" chat room earlier that day. That same

day, Chatstep reported that the user “Dairy” accessed the “Ghotel” chat room via IP address 2601:1c0:8201:53a0:781c:cfd7:5c5b:c3d5 Port #49748 (hereinafter the “SUBJECT IP ADDRESS”).

26. The NZDCET investigator determined the SUBJECT IP ADDRESS was located in the United States. The investigator forwarded the information and related case materials to HSI Phoenix for further investigation. Utilizing a publicly available database, an HSI Phoenix special agent determined that the SUBJECT IP ADDRESS belonged to Comcast.

27. On or about November 13, 2017, HSI Phoenix agents submitted a Department of Homeland Security (DHS) administrative summons to Comcast requesting subscriber information and IP address connection records for the SUBJECT IP ADDRESS on the date and at the time “Dairy” posted the link containing suspected child pornography in the “Ghotel” chat room. On or about November 17, 2017, Comcast provided the following subscriber information for the IP address: 2601:1c0:8201:53a0:781c:cfd7:5c5b:c3d5 Port #49748 on the date and time of the post:

Subscriber Name: Kevin Myers
 Service Address: 2300 NW Rolling Green Dr.
 Apt. 126
 Corvallis, OR 973303974
 Telephone #: 541-752-1035
 Type of Service: High Speed Internet Service
 Account Number: 8778106010559381
 Start of Service: Unknown
 Account Status: Active
 IP Assignment: Dynamically Assigned
 Email user IDs: kev541, jcmgames, kevin2test2, kevonabeach,
 kevm541, cruz2big, kevin2test (All the user ID's end in @comcast.net)

28. HSI Phoenix forwarded the investigative information to HSI Portland. On or about January 29, 2018, I reviewed the provided materials, including the suspected child pornography image files posted by Chatstep user “Dairy.” Descriptions of four of those image files follow:

a. 1ed73bfc576ca32b6f0a5a94e37386e6 (Hash ID): This file depicts a naked prepubescent girl lying on her back on a bed while a naked adult man is on top of her in a missionary sex position. The girl’s legs are wrapped around the man’s back. The man’s face is blocked with a piece of paper. It appears that they are engaging in actual or simulated sexual intercourse. The file also has what appears to be a partial IP address -- “124.150.160” – stamped on the photo.

b. d8a2a8dd5d4ef6c7e73efe9785de1657 (Hash ID): This file depicts a naked prepubescent girl, shown from the chest up, fellating an adult’s penis, which she is holding with her hands. The IP address “124.150.160.21” is stamped on the photo.

c. 3d8875d82f4ff0ec51ca26c9f9d84c0c (Hash ID): This image is a close-up of a toddler’s vagina. In the image, a hand spreads the girl’s vagina while a needle is pierced through her labia majora. The image has a caption that reads “2 years little girl’s torture with needle.” The IP address “124.150.160.21” is stamped on the photo.

d. 0ca589e40210262f7d68d1affaa2f4b2 (Hash ID): This file depicts a prepubescent girl, naked from the waist down, lying on the floor in front an adult male who is also naked from the waist down. The adult man penetrates the girl’s anus with his penis. The IP address “124.150.160.21” is stamped on the photo.

29. Queries conducted in commercial databases indicate that Kevin John MYERS is associated with 2300 NW Rolling Green Dr., Apt 126, Corvallis, Oregon 97330. In addition, MYERS's Oregon driver's license lists an address of 2300 NW Rolling Green Dr., Apt 126, Corvallis, Oregon 97330, and he has two vehicles registered in his name at that address.

30. On or about February 6, 2018, I received information from the U.S. Postmaster that Kevin MYERS and Jordan MYERS receive mail at 2300 NW Rolling Green Drive, Apt. 126, Corvallis Oregon 97330. Jordan Chase MYERS (DOB XX/XX/1994) appears to be Kevin MYERS' son.

31. On February 8, 2018, HSI SA Duffy drove to 2300 NW Rolling Green Dr., Apt. 126, Corvallis, Oregon 97330, and took photographs of the exterior of the residence. The apartment is located in the Forest Green Townhouses complex, which contains multiple two-story townhouse buildings. Each building is taupe in color with a brown and white sign identifying the building number and apartment numbers. Apartment #126 is an end unit on the northwest corner of the building marked "2300." Apartment #126 has a small brown placard with the white numbers "126" in the center of the door at approximately eye level, next to a "no soliciting" placard. The front door to apartment #126 is green, is located on the ground floor, and faces north. Apartment #126 has a small patio area with a sliding glass door immediately to the right of the front door.

32. On that same date, SA Duffy parked on the street in front of the residence and scanned for wireless networks using a mobile device. SA Duffy observed only one unsecured wireless network, called "Xfinitywifi." According to instructions provided by Xfinity WiFi, it is a network of hotspots that allows users to connect to the internet at fast WiFi speeds around town

while saving on user's data plan. To access Xfinity WiFi hotspots, all users must install the Xfinity WiFi app and enter their Xfinity username and password to start browsing or streaming. According to Comcast official, each Xfinity WiFi hotspot user will have a general IP address and an identifying source port referring back to their Comcast account when using Internet Protocol Version (IPV) 4.

33. According to a law enforcement database, neither Kevin MYERS nor Jordan MYERS has a known criminal history. The IP address associated with the "Ghotel" chat room post has not surfaced in other child pornography investigations.

34. On or about February 13, 2018, Pacific Power advised the subscriber for 2300 NW Rolling Green Dr., Apt 126, Corvallis, Oregon 97330 is:

Customer name:	Kevin J. Myers
Telephone:	541-715-5294
Account number:	28637940 001 001
Service dates:	09/06/97- present
Email address:	kevin2test@comcast.net

Search and Seizure of Digital Data

35. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use and who used them.

36. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb

drives, secure digital media used in phones and cameras, personal music devices, and similar items.

Removal of Data Storage Devices

37. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally highly impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a

single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

Laboratory Setting May Be Essential For Complete and Accurate Analysis Of Data

38. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

39. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created,

modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

40. *Latent Data:* Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

41. *Contextual Data:*

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The

browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

42. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, “computer personnel”), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it

contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b. *On site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data that fall within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized

pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

Items to be Seized

43. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers,

electronic notebooks, personal digital assistants, iPods, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies, bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

Retention of Image

44. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

45. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.


46. The government has made no prior efforts in any judicial fora to obtain the materials sought in this requested warrant.

Conclusion


47. Based on the foregoing, I have probable cause to believe that Kevin John MYERS or someone with access to his Internet connection has committed the offenses of transportation, distribution, and possession of child pornography, in violation of 18 U.S.C. § 2252A. I also have probable cause to believe that contraband and evidence, fruits, and instrumentalities of the aforementioned violations, as more fully described in Attachment B hereto, may be located on the person of Kevin John MYERS and at his residence, 2300 NW Rolling Green Drive, Apt. 126, Corvallis Oregon 97330, which is more fully described in Attachment A. I therefore respectfully request that the Court issue a warrant authorizing a search of the person Kevin John MYERS and

his residence for the items listed in Attachment B, and authorizing the examination and seizure of any such items.

48. This affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Gary Sussman prior to being submitted to the Court. AUSA Sussman informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.


Seung Sung
Special Agent
Homeland Security Investigations

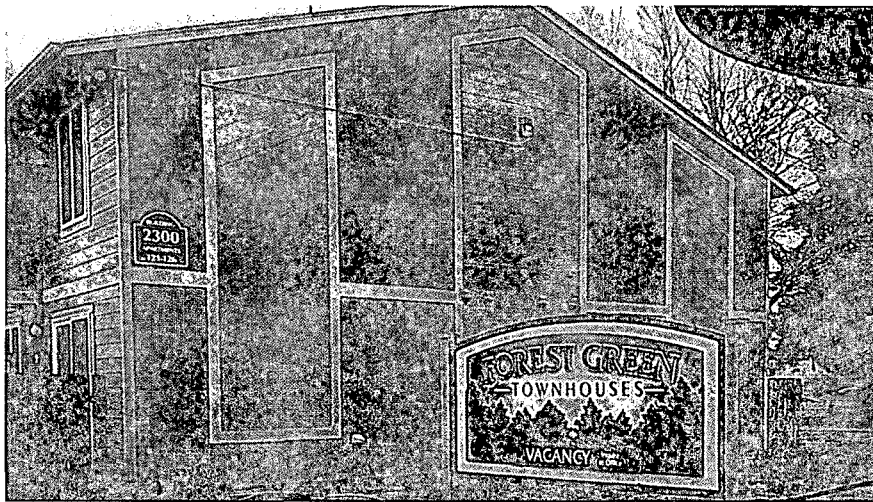
Sworn and subscribed before me this 8th day of March 2018.


Honorable John V. Acosta
United States Magistrate Judge

ATTACHMENT A
Premises to be Searched

**The Person of Kevin John Myers, date of birth XX-XX-1966, and the Premises at
2300 NW Rolling Green Drive, Apt 126, Corvallis, Oregon 97330**

The premises is an apartment located in the Forest Green Townhouses complex, which contains multiple two-story townhouse buildings. Each building is a taupe color with a brown and white sign identifying the building number and apartment numbers. Apartment #126 is an end unit on the northwest corner of the building marked “2300.” Apartment #126 has a small placard with the white numbers “126” in the center of the door at approximately eye level, next to a “no soliciting” placard. The front door to apartment #126 is green, is located on the ground floor, and faces north. Apartment #126 has a small patio area with sliding glass door immediately to the right of the front door.



ATTACHMENT B

Items to be Searched For, Seized, and Examined

The following records, documents, and items that constitute contraband and evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), namely the transportation, distribution, and possession of child pornography:

1. **Records, Documents, and Visual Depictions:**

- a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; and video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;
- d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs.

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, receiving, or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received, and the like.

2. **Digital Evidence:**

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems,

docking stations, monitors, web cams, microphones, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, iPods, and cellular telephones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items, which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data, and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web

browser's history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mail, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

As used herein, the terms "records," "documents," "programs," "applications," or "materials" include records, documents, programs, applications, or materials created, modified, or stored in any form.

Search Procedure

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a) *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will be seized only if it contains data falling within the list of items to be seized as set forth herein.

b) *On-site imaging, if practicable.* If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c) *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d) Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and herein. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e) Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f) If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government

needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

g) If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h) If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.